

REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-6, 8-16, and 18-23 are currently pending, Claim 23 having been added. The changes and additions to the claims do not add new matter and are supported by the originally filed specification, for example, new dependent Claim 23 is supported by at least Fig. 5, and page 24, line 14 to page 26, line 18.

In the outstanding Office Action, the specification was objected to; Claims 1-5, 9-15, 19, and 20-22 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier ("Applied Cryptography," Second Edition) in view of Bo Lin et al. (GB 2345229A, hereafter "Lin") and Obana (U.S. Patent No. 6,970,561); Claims 6 and 16 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Lin, Obana, and Kocher et al. (U.S. Pub. No. 2001/0053220A1, hereafter "Kocher"); and Claims 8 and 18 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Lin, Obana, and Kaminaga et al. (U.S. Pub. No. 2002/0124179A1, hereafter "Kaminaga").

With respect to the objection to the title, Applicants respectfully submit that the present amendment to the title overcomes this ground of objection.

With respect to the rejection of Claim 1 under 35 U.S.C. §103(a), Applicants respectfully traverse this ground of rejection. Claim 1 recites, *inter alia*,

a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second group of the groups, and the first input data to be encrypted for the first group is

generated independently relative to the second input data to be encrypted for the second group, said control section mixing processing sequences of encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group and under a condition in which a processing sequence of the encryption processing units within each of the plurality of groups is fixed;

an encryption processing section configured to perform an encryption process in accordance with the mixed encryption processing sequence set by said control section; and

a transmitting unit configured to transmit each of encrypted output data generated independently by the first group and the second group to an external device.

Applicants respectfully submit that the combination of Schneier, Lin and Obana fails to disclose or suggest all of the features of Claim 1.

As previously presented, Schneier is directed to a description of the Data Encryption Standard (DES) and combining block ciphers. In chapter 12, Schneier describes conventional DES, which includes 16 rounds in which a function which uses a key is applied on a plaintext block 16 times (see pages 270-278 of Schneier). In chapter 15, Schneier then describes ways to combine block algorithms to get new algorithms to increase security without designing a new algorithm. In Chapter 15, Schneier describes Double Encryption and Triple Encryption. In Triple Encryption, a ciphertext block is operated on three times with multiple keys (see pages 357-361 of Schneier). Schneier describes different permutations of Triple Encryption based on the types of keys used (see page 360, describing Triple Encryption with Three Keys and Triple Encryption with Minimum Key). Schneier also describes different modes of Triple Encryption involving Cipher Block Chaining (CBC), such as “Inner-CBC” and “Outer-CBC” (see page 360).

As was previously emphasized by the Applicants, in the Triple Encryption described by Schneier, including both Inner-CBC and Outer-CBC modes, *encryption is being applied to a single plaintext file* (see page 360, for example, where Schneier describes encrypting “the entire file” for each of the Inner-CBC and Outer-CBC modes). Additionally, a single DES with 16 rounds still has just one independently generated input (the initial input), because any subsequent input into any of the later rounds is derived from an input from the previous round. Thus, any one of these processes being described in Schneier constitutes only a single group as defined by Claim 1 because each of the processes described in Schneier is still just directed to a single independently generated input being put through an overall encryption process to produce a single encrypted output.

The Office Action acknowledges this point in indicating that Schneier does not explicitly disclose “a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second group of the groups, and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group.” (See Office Action, at page 5).

The Office Action relies on Lin and Obana to remedy the deficiencies of Schneier with regard to Claim 1.

As previously presented, Lin describes inserting “dummy” S-block lookups into a real DES process (see page 11, lines 10-13). The Office Action relies on such a dummy S-block lookup as corresponding to the claimed “second group” which has an independently generated input from a “first group.” (See Office Action, at page 10). However, Lin explicitly describes the following on page 11, lines 10-15:

Another technique which could be used to improve resistance to attacks is to insert a “dummy” operation to confuse analysis of a power signature. For example, one could insert “dummy S block look-ups into the DES routing, **whereby an S block look-up is performed but**

the result or output of the look-up is not included in the pre-output value, U, but is instead written elsewhere and not used. [Emphasis added].

On the contrary, Claim 1 defines “a transmitting unit configured to transmit each of encrypted output data generated independently by the first group and the second group to an external device.” In other words, in Claim 1 both the “first group” and “second group” are “separate and independent encryption process for encrypting an input data” and since the output of first group and second group are both transmitted to an external device they both have output values *that are used*.

Thus, the dummy S-block of Lin cannot be interpreted to correspond to the “second group” (or the “first group”) as defined by Claim 1, and therefore inserting the dummy S-block lookups of Lin into a process of Schneier as asserted in the Office Action would not achieve all of the features of Claim 1.

The Office Action appears to acknowledge that there is a deficiency in Lin, because it states that the combination of Scheiner and Lin do not explicitly disclose transmitting encrypted data to an external device. (See Office Action, at page 6).

However, Applicants submit that this does not fully state the deficiency of Lin, because the actually deficiency in Lin, as described in detail above, is that the dummy S-block of Lin is not the equivalent of the claimed “first group” or “second group” because an output of the dummy S-block group is not sent to an external device. In other words, the claimed “first group” and “second group” when taken as a whole are explicitly different than a dummy encryption process due to the previous amendments to the claims.

Applicants note that the Office Action relies on Obana to remedy the deficiencies of Scheiner and Lin with regard to Claim 1. (See Office Action, at page 6).

Obana is directed to a method of encryption and decryption with endurance to cryptanalysis methods such as simple power analysis and differential power analysis. Fig. 1 shows a system in which there is an input unit 110 (which supplies plaintext for encryption), an encryption processing unit 120, a storage unit 130, a random number generating unit 140, and an output unit 150 (which outputs encrypted ciphertext). An encryption operating section 121 within the encryption processing unit 120 performs encryption via a plurality of processing stages (see col. 12, lines 5-6). In the first embodiment of Obana, the necessary data in each encrypting stage of the encrypting operation is changed depending on random numbers (see also Fig. 2). This makes it difficult to perform a power analysis on the system because it is difficult to determine whether or not the change of power consumption is caused based on the data needed in the actual encrypting operation. Thus, Obana does not resist power analysis by mixing two separate independent encryption processes, which have their own independent input and output. On the contrary, Obana resists power analysis by changing the data used in a single independent encryption process, which has input 110 and output 150, depending on generated random numbers.

Therefore, while the Office Action cites to Obana as disclosing “transmitting an encrypted data to external device wherein encrypting and/or decrypting operation based on a random number,” (see Office Action, at page 6), this disclosure does not remedy the deficiencies of Schneier and Lin. As discussed above, a dummy S-block group of Lin is being interpreted as the claimed “second group” because the dummy S-block look-ups are inserted into an encryption process. However, the dummy S-block group falls short of being the claimed second group because they by themselves do not represent an independent encryption process that provides an encrypted output to an external device. Therefore, to remedy this deficiency, Obana would have to disclose transmitting *the output of a dummy encryption process* to an external device. However, Obana does not make such a disclosure

and merely recites an encryption process with a single input and single output. A person of ordinary skill in the art would not look at the disclosure of Obana *and then decide to transmit the output of a dummy encryption process to an external device* because that would be totally contrary to the purpose of a **dummy** encryption process. Also, there is no disclosure in Obana to take its non-dummy encryption processing units from an independent encryption processing sequence and mix them with encryption processing units from another independent encryption processing sequence.

MPEP §2142 states:

The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in *KSR International Co. v. Teleflex Inc.*, 550 U.S. 82 USPQ2d 1385, 1396 (2007) noted that **the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit**. The Federal Circuit has stated that "rejections on obviousness cannot be sustained with mere conclusory statements; instead, **there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness**." In re Kahn, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006). (Emphasis added).

Therefore, for all the reasons discussed above, the Office Action has not provided any explicit reasoning as to why the disclosure of Obana would allow a person of ordinary skill in the art to modify the combination of Schneier and Lin to achieve all of the features of Claim 1 discussed above.

Thus, Applicants submit that Claim 1 (and all associated dependent claims) patentably distinguishes over Schneier, Lin, and Obana, either alone or in proper combination.


Kocher and Kaminaga have been considered but fail to remedy the deficiencies of Schneier, Lin, and Obana with regard to Claim 1. Thus, Applicants respectfully submit that Claim 1 (and all associated dependent claims) patentably distinguishes over Schneier, Lin, Obana, Kocher, and Kaminaga, either alone or in proper combination.

Independent Claims 9, 11, 19, 21, and 22 recite features similar to those of Claim 1. Thus, Applicants respectfully submit that Claims 9, 11, 19, 21, and 22 (and all associated dependent claims) patentably distinguish over Schneier, Lin, Obana, Kocher, and Kaminaga, either alone or in proper combination.

Consequently, in light of the above discussion and in view of the present amendment, the outstanding grounds for rejection are believed to have been overcome. The present application is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested. Furthermore, the examiner is kindly invited to contact the Applicants' undersigned representative at the phone number below to resolve any outstanding issues.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 08/07)

Sameer Gokhale
Registration No. 62,618